

December 7, 2018

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Dear Director Krebs:

I am writing to understand what progress the Department of Homeland Security (DHS) has made in addressing the threat of malicious software delivered to federal computers through internet advertisements.

One year ago, on November 16, 2017, I wrote to then-White House Cybersecurity Coordinator, Rob Joyce, regarding the threat posed by foreign government hackers using online advertisements to deliver malware to the computers of federal workers. In that letter, I urged the administration to direct DHS to require federal agencies to block delivery of all internet ads containing executable computer code to employees' computers. In its response on April 20, 2018, DHS stated that it was continuing to investigate these risks and working with representatives from the online advertising industry to address this threat.

In June 2018, the National Security Agency (NSA) issued public guidance related to the threat posed by malicious advertisements. In the attached document, which NSA published on its website, the agency observed that "advertising has been a known malware distribution vector for over a decade" and as such, the agency recommends that organizations address this risk "by blocking potentially malicious, internet-based advertisements."

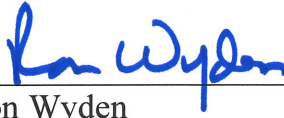
In light of the NSA's public confirmation of the threat posed by internet advertising-delivered malicious software, I would appreciate an update on DHS' progress on this issue. Please also provide me with answers to the following questions by January 30, 2019:

1. Does DHS agree with NSA's assessment that "Cyber adversaries can leverage malicious advertising ('malvertising') to install malware?"

2. Does DHS agree with NSA's recommendation that organizations "address malvertising by blocking potentially malicious, internet-based advertisements?"
3. Does DHS currently block internet-based advertisements on its own network?
4. What steps, if any, has DHS taken to recommend that federal agencies block internet-based advertisements?

I appreciate your attention to this important matter. If you have any questions, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator

CC: General Paul M. Nakasone, Director, National Security Agency



NATIONAL SECURITY AGENCY CYBERSECURITY INFORMATION

BLOCKING UNNECESSARY ADVERTISING WEB CONTENT

Cyber adversaries can leverage malicious advertising (“malvertising”) to install malware. Exploit kits in malicious ads can take advantage of unpatched vulnerabilities to silently install malware¹. Administrators should ensure that software updates are implemented promptly to prevent malware installation. Blocking potentially malicious web advertisements further mitigates malvertising. Additionally, blocking such content can decrease traffic across the network boundary, streamlining incident forensics and enhancing network performance.

BACKGROUND

Web browsers present a major cyber security risk due to their frequent interaction with untrusted, Internet-based content. Due to the vast Internet landscape, it is generally not possible to predict and catalog the “good” websites that a user may visit. Instead, blacklisting approaches (such as Microsoft® SmartScreen² and Google Safe Browsing™³) enhance security by blocking known malicious websites. Content that is neither inherently useful nor known to be malicious in nature, such as advertisements, often go unrestricted. Many websites include space for third party advertisers to display content. Despite the benign nature of most advertising content, advertising has been a known malware distribution vector⁴ for over a decade⁵. This attack, known as “malvertising,” allows a malicious actor to target users based on location, interests, browsing habits, and system specific identifiers, such as software versions¹.

RECOMMENDATION

Organizations which have already implemented a comprehensive and rapid patching regime⁶ can further address malvertising by blocking potentially malicious, internet-based advertisements. While both network and host based solutions are outlined below, network-based solutions provide a similar level of protection to host solutions without introducing additional risk.

There are a variety of advertisement blocking strategies with significant differences in user impact, cost, and infrastructure requirements. Administrators should use this guidance to determine the best strategy for their environment based on existing network infrastructure.

AD-BLOCKING THROUGH NETWORK FUNCTIONS

Blocking access to advertisements at the network boundary can often be achieved using technologies already deployed on the network. Many firewalls and DNS servers provide the necessary building blocks to implement the end goal. An organization can choose to incorporate more than one of the below network implementations depending on the feature set of the deployed systems.

¹ *I'll Make You an Offer You Can't Refuse* (2017-01-04). <https://ncsc.gov.uk/blog-post/ill-make-you-offer-you-cant-refuse>

² Microsoft and SmartScreen are registered trademarks of Microsoft Corp.

³ Google Safe Browsing is a trademark of Google, Inc.

⁴ *Weekly Threat Report* (2017-06-02). <https://ncsc.gov.uk/report/weekly-threat-report-2nd-june-2017>

⁵ *Malvertising* (2007-12-06). William Salusky SANS ISC. <https://isc.sans.edu/diary/Malvertising/3727>

⁶ *Security Configuration Guide for Browser Updates* (2016-10-25). <https://www.iad.gov/iad/library/ia-guidance/security-configuration/applications/security-configuration-guide-for-browser-updates.cfm>

General Network Solutions

Some boundary products like firewalls and proxies provide universal resource locator (URL) classification engines as part of an Intrusion Prevention Service. These products have domains organized into categories, which are either defined by the vendor themselves or can be subscribed to from a third-party vendor. The firewall will then perform an action based on pattern matches; an example would be blocking the client request for the ad domain, which would generate a TCP reset.

This solution requires the least amount of custom engineering due to the native functionality provided in IT products. However, if this service was not purchased, there exist freely available solutions described below.

DNS Servers

Domain Name System (DNS) servers are an effective means of blocking publicly-known advertising domains due to advertisers' reliance on domain name lookups. To accomplish DNS ad-blocking, organizations should first ensure that all DNS requests are routed through corporate DNS servers. A firewall rule denying DNS traffic except through corporate servers ensures that misconfigured systems cannot bypass ad-blocking protection.

Publicly-available ad server lists generally need to be transformed because they were primarily designed for use with host-based software. Because of this, organizations can maintain granular control of the internally hosted list. It is important to note that these types of lists are managed by a community of enthusiasts, and additional work may be needed to obtain broader coverage.

Ingesting these lists will require the parsing of domain names from each line. NSA recommends that network administrators script the downloading, parsing, and formatting of a reputable, public advertiser list to maintain a current advertiser list. This parsed list can be utilized in the firewall solution above if it is determined that the commercial list is missing domains.

Response Policy Zones (RPZ) allow DNS Servers to substitute query answers. When using RPZ, it is recommended to follow the walled garden approach⁷ by returning a canonical name (CNAME) to an internally owned webserver that will serve minimal content to the end user. This will ensure that web requests do not hang while waiting for a response. However, a black-hole approach is not discouraged.

If RPZ is not implemented in your organization's DNS server, then standard Forward Lookup Zones can be defined for each domain to be altered, and a black-hole IP address should be returned. A boundary device upstream should then reset the connection so the client's connection does not hang waiting for resources to load.

ADVERTISEMENT BLOCKING AT THE HOST LEVEL

Host Based Ad-Blocking

Some Host/Endpoint-level security systems offer ad-blocking functionality that is bundled with or readily deployed from enterprise endpoint security implementations. Organizations may be able to leverage ad-blocking software provided by solutions already within their infrastructure.

Because of their privileged position in the operating system, endpoint ad-blockers can filter content by blocking DNS requests or HTTP requests to known advertising domains or IP addresses. Some systems implement their ad-blocking as a browser extension, which is described in greater detail below.

Ad-Blocking Browser Extensions

Web based advertisements are primarily targeted at web browsers and browser extensions can block such content. Browser extensions are able to incorporate some detection techniques infeasible at the network layer, such as de-obfuscation and behavioral heuristics. However, some of these extensions adopt a free-to-use business model that generates revenue by collecting user information and browsing data. Because browser extensions operate at a privileged level in the browser environment, they have access to most data entering and exiting the browser. Implementing a malicious ad-blocking extension should be done with considerable caution. Such software could cause a greater compromise to network security than a malvertising attack, even when installed from reputable browser app stores⁸.

⁷ Walled Garden for Remote Access (2015-10). <https://ncsc.gov.uk/guidance/walled-garden-remote-access-architectural-pattern-2>

⁸ Over 20 million Users Installed Malicious Ad Blockers From Chrome Store (2018-04-19). <https://thehackernews.com/2018/04/adblocker-chrome-extension.html>

AD-BLOCKING CONCERNS

Breaking Webpage Dependencies

Some websites restrict content if an ad-blocker is detected. Though this is currently a rare practice, it could prevent users from accessing legitimate, useful web content. If ad-blocking is implemented at the host level, the user may have the ability to temporarily permit ads allowing access to the desired content. Ad-blocking implemented at the network level, however, does not provide users with an immediate means to access the protected content. Depending on how ad-blocking is implemented, administrators should ensure that users are trained on adding exceptions to host based ad-blocking or are aware of potential content degradation when network based ad-blocking occurs. Most ad-blockers allow administrators to whitelist specific domains if ad-blocking is hindering a mission essential resource.

Malicious Denial of Service Attacks

Ad-blocking is accomplished through the use of domain/IP blacklists that are frequently updated by communities of individuals. These lists may not be well-vetted by the ad-blocking vendor themselves creating the potential for untrusted individuals to introduce non-advertisers to the blacklist. In extreme cases, a malicious user could list reputable domains (such as *.mil) as known advertisers which could cause the ad-blocker to deny mission critical communications with those domains. To counter this threat, system administrators should whitelist regularly used or highly trusted domains within the ad-blocking software. Care should be taken not to override blacklists that may match these rules. Suggested whitelisting for government customers includes:

- Trusted top level domains: *.mil, *.gov, *.edu
- Operating System vendors (such as *.microsoft.com and *.apple.com)
- Productivity websites used by the organization (such as *.office.com and *.salesforce.com)
- Internal/external organization websites and websites regularly used by the organization

Careful establishment of such a whitelist will greatly reduce the denial of service risk from malicious ad-blocking contributors.

Incomplete Advertiser Coverage

Due to the increasing impact of ad-blocking lists to advertisers, some ad-blockers have productized domain whitelisting. Advertisers can pay these ad-blockers to remove domains from their known advertiser list. When this occurs, products using the lists will no longer block malvertising attacks from these domains. Administrators are encouraged to use reputable advertiser lists which do not engage in the "pay to advertise" practice.

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov